CERTSWARRIOR

GIAC
GSOC
GIAC Security Operations Certified

Questions&AnswersPDF

ForMoreInformation:
https://www.certswarrior.com/

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.1

Question: 1

What advantage does integrating a Threat Intelligence Platform with a SIEM offer to a SOC?
Response:

A. It allows the SOC to broadcast threat alerts on television.
B. It enables correlation of external threat data with internal event data for enhanced analysis.
C. It transforms the SIEM into an autonomous AI entity.
D. It provides a direct marketing channel to potential clients.

Answer: B

Question: 2

Which of the following best describes the concept of 'orchestration' in cybersecurity?
Response:

A. The manual process of responding to incidents one by one
B. The coordination of various security tools and processes to work together effectively
C. The elimination of all automated tools to enhance human skillsets
D. Focusing solely on external threats without considering internal processes

Answer: B

Question: 3

Why is it important for Blue Teams to continuously update and refine their automation workflows?
Response:

A. To keep pace with the rapidly changing threat landscape
B. To ensure that workflows become increasingly complex and harder to understand
C. To reduce their reliance on technology in favor of manual processes
D. To increase the time spent on each incident for thorough investigation

Answer: A

Question: 4

During the sharing phase of analytics, what is an effective practice for fostering understanding and engagement among stakeholders?
(Choose Three)
Response:

A. Utilizing interactive visualizations
B. Providing detailed technical documentation to all stakeholders regardless of their background
C. Tailoring the presentation to the audience's level of expertise
D. Offering actionable insights based on the data
E. Limiting access to data to prevent information overload

Answer: A,C,D

Question: 5

Which two key practices are essential for continually improving existing analytics solutions?
(Choose Two)
Response:

A. Isolating the analytics team from other departments
B. Incorporating end-user feedback to refine analytics
C. Regularly updating the dataset with new and relevant information
D. Focusing solely on enhancing the visual appeal of reports

Answer: B,C

Question: 6

In the context of SSH, what is a common attack method?
(Choose Three)
Response:

A. Brute force attacks to guess passwords
B. ICMP tunneling to hide communications
C. Man-in-the-middle attacks to intercept data
D. Exploiting vulnerabilities in older SSH versions
E. Using SMTP to intercept SSH keys

Answer: A,C,D

Question: 7

When securing endpoints, which two measures are effective in preventing unauthorized access?
(Choose Two)
Response:

A. Enabling auto-run features for external media
B. Implementing full disk encryption
C. Applying strong, unique passwords for each endpoint
D. Allowing users to install their applications to ensure they have tools they prefer

Answer: B,C

Question: 8

When analyzing HTTP(S) traffic, which two elements are crucial to identify potential attacks?
(Choose Two)
Response:

A. The User-Agent header to determine the browser used
B. Unusually long URLs that may indicate a buffer overflow attack
C. Frequent requests to non-existent pages, possibly indicating a scanning attack
D. The Accept-Language header for localization preferences

Answer: B,C

Question: 9

When monitoring network traffic, which two protocols should be scrutinized for signs of data exfiltration?
(Choose Two)
Response:

A. SSH
B. ICMP
C. SMTP
D. DHCP

Answer: A,B

Question: 10

For analytics enrichment, why is it vital to understand the origin and nature of the data sources?
Response:

A. To ensure the enrichment process adds no value
B. To validate the relevance and reliability of the data
C. To make the data look more complex
D. To focus solely on internal data sources

Answer: B

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ